

REMARKS

Upon entry of the present amendment, claims 8, 10-12, 16-19, and 21-26 will remain pending in this application. Applicant notes that the instant Office Action states that claims 1 and 5-7 are currently pending, but respectfully submits that claims 1 and 5-7 were cancelled in the amendment filed June 27, 2008. Claims 1-7, 9, 13-15, and 20 were previously canceled. Applicant respectfully submits that no new matter is added by the present amendment. In particular, Applicant respectfully submits that the subject matter added to claim 19 is supported in the Specification at least at page 27, lines 23-24 (“any conditions that may be imposed on those rights”) and page 26, lines 4-7 (“if the recipient does not have the right to copy or print the content 32, the trusted component 38 would direct the email application to support such functions with respect to such content 32.”).

Claims 8, 10, 12, 16-17, 19, 21, and 23-25 are understood to stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over U.S. Patent No. 6,856,686 (“DiSanto et al.”) in view of U.S. Patent Application Publication No. 2002/0002674 (“Dabbish et al.”). Claims 11, 18, 22, and 26 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over DiSanto et al. in view of Dabbish et al. and further in view of U.S. Patent No. 5,903,723 (“Beck et al.”).

Claim Rejections Under 35 U.S.C. § 103(a)

Claims 8, 10, 12, 16-17, 19, 21, and 23-25 are understood to stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over DiSanto et al. in view of Dabbish et al. As per claim 8, the rejection is understood to be based in part on the premise that Dabbish et al. discloses digital rights management of restricted content and further discloses forwarding the retrieved rights data to a rights management server, such rights management server for determining that the recipient is an entity listed in the rights data and issuing to the recipient a license corresponding to the protected content to the recipient based on the rights data, such license specifying rights the recipient has with respect to the protected content as determined from the rights data and also including the decrypted decryption key from the rights data; reviewing the issued license to determine that the recipient has a right to render the protected content of the attachment portion of the email; retrieving the decryption key from the license;

and rendering the content. Dabbish et al. is alleged to disclose these limitations at least at claims 1-3. DiSanto et al. is stated as failing to explicitly disclose these limitations.

Applicant makes no admission that Dabbish et al. is prior art under 35 U.S.C. § 102(e). Applicant notes that Dabbish et al. was filed on March 31, 2003. While this date is before the filing date of the instant Application (June 27, 2003), Applicant reserves the right to later submit evidence that the invention date of the currently pending claims predates the filing date of Dabbish et al., thereby disqualifying Dabbish et al. as prior art. However, for the purposes of these remarks, Applicant assumes *arguendo* that Dabbish et al. qualifies as prior art.

Applicant respectfully traverses the rejection. Even assuming *arguendo* that Dabbish et al. qualifies as prior art, Applicant submits that Dabbish et al. fails to disclose the limitations of claim 8 that are admittedly not disclosed by DiSanto et al. Fig. 3 and paragraph [0031] of Dabbish et al. disclose a digital rights management system that uses a communication system with trust identification capabilities. Paragraph [0031] states that “when content is transported between [electronic devices], there is a need to establish trustworthiness of the receiving device.” Paragraph [0023] gives an example of the need to establish trustworthiness in the DRM context: “if electronic device 102 had a desire to transfer digital content to electronic device 103, the trustworthiness of electronic device 103 should be verified prior to making the transfer . . . to ensure that the receiving device 103 does not perform illegal operations on the protected content. For example, a compromised (broken) device might copy the unprotected digital content for distribution on the Internet or, less severely, give false information about the number of copies made or times the content has been accessed.” Fig. 6 and paragraphs [0035]-[0043] disclose the operation of an electronic device that determines the trustworthiness of another electronic device.

However, while Figs. 3 and 6 and the corresponding portions of the Specification of Dabbish et al. disclose determining the trustworthiness of an electronic device, Applicant does not understand Dabbish et al. to disclose “a rights management server . . . for determining that the recipient is an entity listed in the rights data and issuing to the recipient a license corresponding to the protected content based on the rights data.” Rather, in Dabbish et al., while the electronic device may periodically update its internal database to retrieve status information for other electronic devices as disclosed at paragraph [0025], there are at

least two significant differences between the operation of the system in Dabbish et al. and the method recited in claim 8. First, in Dabbish et al., the electronic device does not contact the certificate authority to determine whether another electronic device is trustworthy. Rather, as disclosed at least at paragraphs [0016]-[0018] of Dabbish et al., each electronic device stores a local database that is used to make this determination. As disclosed at paragraph [0018], “[b]ecause a database of trusted devices exists locally to each device wishing to transfer content, the need to contact a remote server (e.g., content authority) is greatly reduced.” Similarly, the certificate authority in Dabbish et al. does not issue licenses. Rather, as disclosed at paragraphs [0038]-[0043] of Dabbish et al., if it is determined that a proposed recipient is trustworthy, the first electronic device decrypts the DRM protected content, re-encrypts it, and sends the encrypted content to the recipient. The recipient then decrypts and renders the content.

Further, claim 8 recites the limitation “rights data setting forth each entity that has rights with respect to the protected content, and for each such entity a description of such rights.” DiSanto et al. is cited as disclosing this limitation at column 12, lines 39-48, column 13, lines 30-35, and column 13, line 62, to column 14, line 29. Applicant’s review of DiSanto et al. suggests that the cited portions disclose transmission of secure email attachments to multiple recipients by including an appropriately encrypted version for each intended recipient. However, it is not seen where DiSanto et al. discloses rights data that sets forth entities that have rights with respect to the protected content and, for each such entity, a description of such rights. Even if one could construe the list of recipients as a list of entities that are intended to access protected content attached to an email message, the system of DiSanto et al. would allow each recipient to decrypt its respective encrypted version and, following such decryption, have no limitations on its access to or distribution of the protected content. Accordingly, a list of recipients cannot reasonably be construed as describing the rights that each entity has with respect to the protected content.

Based at least on the above remarks, Applicant respectfully submits that claim 8 is patentable over DiSanto et al. in view of Dabbish et al. Claim 10 depends from claim 8 and is also patentable over DiSanto et al. in view of Dabbish et al. at least by reason of this dependency.

Independent claims 12, 19, and 23 all recite a rights management server that receives rights data from an email and that issues a license based on the rights data. As discussed above in connection with claim 8, in Dabbish et al., the electronic device does not contact the certificate authority to determine whether another electronic device is trustworthy; this determination is made with reference to a database stored locally at the electronic device. Accordingly, in Dabbish et al., no email is sent that contains rights data and that is received by a rights management server. In addition, claims 12, 19, and 23 recite rights data as discussed above in connection with claim 8. Therefore, for at least the reasons discussed above in connection with claim 8, claims 12, 19, and 23 are patentable over DiSanto et al. in view of Dabbish et al.

In addition, claim 19 has been amended to recite the further limitations “the rights data setting forth each entity that has rights with respect to the protected content, and for each such entity a description of such rights and a description of conditions imposed on such rights” and “wherein if it is determined that the recipient does not have the right to print the protected content of the attachment portion of the email, print functionality is disabled with respect to the protected content.” Applicant respectfully submits that the cited art does not disclose these limitations. For example, as discussed above in connection with claim 8, the recipient list in DiSanto et al. does not contain a description of rights, let alone a description of conditions imposed on those rights. Further, it is Applicant’s understanding that, in both cited references, once the file is decrypted by the recipient, there is no further limitation as to what the recipient can do with the protected content. Thus, Applicant submits that these added limitations further define the claimed invention above the cited art.

Claims 16-18 depend from claim 12, claims 21-22 depend from claim 19, and claims 24-26 depend from claim 23. These dependent claims are all patentable over DiSanto et al. in view of Dabbish et al. at least by reason of their dependency from the respective independent claims.

Claims 11, 18, 22, and 26 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over DiSanto et al. in view of Dabbish et al. and further in view of Beck et al. The rejection is understood to be based on the premise that Beck et al. teaches compressing attachments for the purpose of minimizing storage space for transmitting to a recipient. However, Beck et al. does not disclose, and is not alleged in the instant Office Action to

DOCKET NO.: 304791.1 / MSFT-2152
Application No.: 10/607,898
Office Action Dated: September 19, 2008

PATENT

disclose, the other limitations of the independent claims that are also not disclosed in either DiSanto et al. or Dabbish et al. Accordingly, Applicant submits that claims 11, 18, 22, and 26 are patentable over DiSanto et al in view of Dabbish et al. and further in view of Beck et al. at least by reason of their dependency from claims 8, 12, 19, and 23, respectively.

Based at least on the above remarks, Applicant respectfully submits that the currently pending claims are patentable over the cited art and requests reconsideration and removal of the rejections under 35 U.S.C. § 103(a).

DOCKET NO.: 304791.1 / MSFT-2152
Application No.: 10/607,898
Office Action Dated: September 19, 2008

PATENT

CONCLUSION

In view of the above amendments and remarks, Applicant respectfully submits that the present application is in condition for allowance. Reconsideration of the application is respectfully requested.

Date: December 19, 2008

/Kenneth R. Eiferman/

Kenneth R. Eiferman
Registration No. 51,647

Woodcock Washburn LLP
Cira Centre
2929 Arch Street, 12th Floor
Philadelphia, PA 19104-2891
Telephone: (215) 568-3100
Facsimile: (215) 568-3439